Chapitre IV

Sécurité système

Abdelali Saidi

abdelali.saidi@gmail.com

1. Menaces à la sécurité du système
2. Bases de la sécurité du système
3. Sécuriser un système Linux
   - La sécurité locale
   - Sécurisation des applications

Plan

1. Menaces à la sécurité du système
2. Bases de la sécurité du système
3. Sécuriser un système Linux
   - La sécurité locale
   - Sécurisation des applications

Menaces à la sécurité du système

Infections

Comme une infection de l'organisme, une infection est définie par l'opération d'un agent externe malveillant. Ces organismes malveillants peuvent être présents sous différentes formes:

- Virus
- Worms
- Spywares
- Trojans
- Rootkits

Menaces à la sécurité du système

Intrusions

Une intrusion est une pénétration Interdire sur un système. Elle peut être le résultat de backdoors, ou une faiblesse sur le système.

Plan

1. Menaces à la sécurité du système
2. Bases de la sécurité du système
3. Sécuriser un système Linux
   - La sécurité locale
   - Sécurisation des applications

Bases de la sécurité du système

Outils de sécurité système

- Antivirus
- Antispywares
- Antirootkits
- Vulnerability scanner
- Patch/update management

Bases de la sécurité du système

Disponibilité du système

- Clustering: Un cluster est un groupe de plusieurs ordinateurs reliés entre eux pour former une entité unique appelée un noeud. Il existe deux principaux types de clusters:
  - HA clusters
  - Distributed calculation / grid or cloud computing
- Load balancing
- Hardware redundancy
- Hot swapping

Bases de la sécurité du système

La sauvegarde de donnée

Les sauvegardes permettent de stocker des données et d'éviter les suppressions ou les pertes non-désirées.

- Les sauvegardes doivent être programmées périodiquement
- Les sauvegardes sérieuses doivent être mises sur des bandes magnétiques
- Les sauvegardes précieuses doivent être mises sur des datacenter

RAID (Redundant Array of Inexepensive Disks) permet d'augmenter la disponibilité des données par des mécanismes de redondance et de sécurité.

Plan

1 Menaces à la sécurité du système
2 Bases de la sécurité du système
3 Sécuriser un système Linux
- La sécurité locale
- Sécurisation des applications

La sécurité locale

La commande sudo

Cette commande permet à un compte ordinaire d'exécuter des commandes nécessitant les privilèges du root.

- Exemple : sudo useradd login
- /etc/sudoers : contient les utilisateurs qui ont le droit d'utiliser la commande sudo (Exemple : *login ALL = (root) [NOPASSWD:] /usr/bin/useradd, /usr/bin/usermod*)

La connexion

Commandes

- who : liste des utilisateurs actuellement connectés
- last : liste des dernières connexions qui ont abouti
- lastb : liste des dernières connexions qui ont échoué
- lastlog : liste de tous les utilisateurs et leur dernière connexion

Les fichiers

- /etc/passwd : les utilisateurs
- /etc/group : les groupes
- /var/log/wtmp : l'historique des connexions
- /var/log/utmp : la liste des utilisateurs actuellement connectés
- /var/log/btmp : l'historique des connexions ayant échouées

Les mots de passe

Les bonnes pratiques

- changer les mots de passe régulièrement
- ne pas taper le mot de passe dans la présence d'autrui
- ne jamais l'écrire sur papier
- ne pas transmettre le mot de passe par téléphone ou par e-mail

Ce qu'il faut faire

- jouer sur la longueur du mot de passe
- aléatoire et facile à mémoriser
- utiliser des minuscules et des majuscules
- utiliser des chiffres et des caractères spéciaux aussi
- possibilité de le taper rapidement

Les mots de passe

Ce qu'il ne faut pas faire

- utiliser des mots qui ont un rapport avec vous
- utiliser des mots du dictionnaire
- des suites de lettres célèbres
- un mot à l'envers
- utiliser le mot de passe par default

Génération du mot de passe

- prendre les initiales d'une phrase
- mélanger plusieurs mots
- une suite de caractères facile à retenir

Les mots de passe

Commandes

- passwd : modifie les mots de passe
- chpasswd : modifie les mots de passe par lot
- chage : modifie les informations de validité d'un mot de passe
- john : essaye de craquer les mots de passe
- pwconv : extrait les mots de passe de /etc/passwd et les met dans /etc/shadow
- pwunconv : fait l'inverse de la commande précédente

fichiers

- /etc/passwd
- /etc/shadow
- /etc/login.defs

La sécurité pour les utilisateurs

Règles de sécurité

Par exemple :

- Choisir un bon mot de passe
- Ne pas saisir son mot de passe si on est surveillé
- Le répertoire de connexion doit être privé
- Définir un UMASK restrictive
- Ne jamais abandonner son terminal sans se déconnecter
- Restreindre les droits sur le fichier .bash_profile

Commandes

- vlock : vérrouille le terminal courant
- umask : change le umask

Variable d'environnement

- TMOUT : la durée d'inactivité au bout de laquelle la déconnexion aura lieu

Les droits d'accès

Catégories d'utilisateurs

Lors de l'accès à un fichier, le noyau considère trois catégories d'utilisateurs pour ce fichier:

- L'utilisateur propriétaire (u)
- Les membres du groupe propriétaire (g)
- Les autres utilisateurs (o)

Les droits

Droit/type	fichier ordinaire	répertoire
read (r)	lecture du contenu	lister son contenu
write (w)	modification	créer et supprimer du contenu
execute (x)	exécuter le fichier	accéder au contenu

Les droits d'accès

Droits spéciaux

- Le sticky bit : sur un répertoire, tous les utilisateurs qui ont droit de modification sur ce répertoire ne pourront modifier que ce dont ils sont propriétaires
- Le Set-UID : sur un fichier exécutable, il permet de l'exécuter avec les privilèges de son propriétaire
- Le Set-GID : sur un répertoire, il permet de passer le groupe propriétaire au contenu nouvellement créé dans ce répertoire

Les ACL

Présentation

Une ACL permet de positionner une liste de contrôle d'accès associée à un fichier. Chaque élément de la liste détermine l'utilisateur et les droits dont il bénéficiera sur ce fichier

Caractéristiques

- Les ACL sont prioritaire sur les droits d'accès
- La notion de masque d'ACL permet de savoir si l'ACL doit être prie en compte en partie, en totalité ou bien ignoré
- La gestion des ACL est délicate, les ACL par default simplifie les choses
- getfacl : visualise les ACL d'un fichier
- setfacl : gère les ACL d'un fichier

Chroot

Présentation

L'appel système chroot() permet de changer le répertoire racine du processus courant.

Serveur Apache

Présentation

La sécurisation du serveur web Apache passe par plusieurs lignes de défense:

- Les droits
- Liaisons chiffrées
- L'authentification des utilisateurs
- Restreindre l'accès aux pages Web
- L'utilisation d'applications sécurisées
- L'audit

L'e-mail

Présentation

Sécuriser le courrier électronique revient à :

- Sécuriser le serveur de messagerie
- Sécuriser les transactions
- Sécuriser le courrier lui même (confidentialité et signature)
- Sécuriser la boite aux lettres (spam, courrier transportant des virus)